

Risk-Based Translator

A risk-based approach shouldn't be specific to a single risk function, but rather applied across interspersed groups and silos within an organization.

Approaching each process owner with the same plan can result in several different interpretations of what the problem is and what various process owners need to do next.

As risk managers reach out to the various departments in their organization, it's best they speak the language of each respective silo. In principal, there are only five things that need to be communicated: 1) Governance, 2) Assess, 3) Mitigate, 4) Monitor, 5) Events.

Use our Risk-Based Translator to introduce a uniform way to talk about risk across your organization.

Information Security

Application/Asset Inventories	= Governance
Vulnerability Analysis	= Assess
Controls	= Mitigate
Testing/Scans	= Monitor
Security Breaches	= Events

Compliance

Requirement Repository	= Governance
Applicability & Adherence Review	= Assess
Policies & Controls	= Mitigate
Reporting	= Monitor
Incidents of Non-Compliance	= Events

Vendor Management

Vendor Inventory	= Governance
Vendor Due Diligence	= Assess
Contract Management	= Mitigate
Service Level Performance	= Monitor
Vendor Breaches	= Events

Financial Reporting

Assertions	= Governance
Materiality	= Assess
Controls	= Mitigate
Testing	= Monitor
Audits	= Events

Business Continuity

Resource Inventory	= Governance
Impact Analysis	= Assess
Event Planning	= Mitigate
Walk-Through Exercises	= Monitor
Disaster Recovery	= Events

Incident Management

Incident Forms and Policies	= Governance
Prioritization	= Assess
Prevention	= Mitigate
Testing	= Monitor
Incident Response	= Events

Policy Management

Policy Inventory	= Governance
Criticality & Applicability	= Assess
Controls & Procedures	= Mitigate
Testing	= Monitor
Non-Conformances	= Events

Audit

Audit Universe	= Governance
Scoping	= Assess
Controls	= Mitigate
Sample Testing	= Monitor
Findings	= Events